

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION**

UNITED STATES OF AMERICA,	:	Case No. 1:16-cr-51
	:	
vs.	:	Judge Timothy S. Black
	:	
ERIC MICHAEL SCHUSTER,	:	
	:	
Defendant.	:	

**ORDER DENYING  
DEFENDANT’S MOTION TO SUPPRESS**

This criminal case is before the Court on Defendant’s motion to suppress evidence (Doc. 29) and the parties’ responsive memoranda (Docs. 31, 32). The Court held oral arguments on January 23, 2017. (Min. Entry, Jan. 23, 2017).<sup>1</sup>

**I. BACKGROUND**

On May 18, 2016, Defendant Eric Michael Schuster was charged in a three-count indictment with: production of child pornography, in violation of 18 U.S.C. § 2251(a), (e) (Count 1); receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2), (b)(1) (Count 2); and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4), (b)(2) (Count 3). (Doc. 14).

Defendant moves to suppress the evidence against him in the instant case, arguing that the evidence was obtained as a result of a search warrant that is “void for want of jurisdiction.” (Doc. 29 at 1).

---

<sup>1</sup> At the Court’s request, a transcript of the evidentiary hearing was prepared and docketed on February 6, 2017. (Doc. 33). Given the importance of the transcript for purposes of preparing this Order, the Court considers the motion to have come ripe for decision following receipt of the transcript.

In or around September 2014, federal agents began investigating a website known as Playpen (“Playpen” or “Website A”). (Doc. 29, Ex. 3 at ¶ 11; Doc. 31 at 3). Playpen served as an online global forum “dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children.” (Doc. 29 at 2).<sup>2</sup> Playpen allowed individuals to register as users, and thereby gain access to the website’s content, including approximately 100,000 postings containing images and videos of child pornography, as well as forums dedicated to discussing how to perpetrate child abuse. (*Id.*, Ex. 3 at ¶ 11; Doc. 31 at 3-4). By March 2015, Playpen had nearly 215,000 registered users.<sup>3</sup> (Doc. 29, Ex. 1 at ¶ 13).

Playpen operated on an anonymous network known as The Onion Router (“Tor”). (Doc. 29 at 2; Doc. 31 at 4). Tor creates anonymity by masking a user’s Internet Protocol (“IP”) address, which could otherwise be used to identify the user.<sup>4</sup> (*Id.*) And while Tor may serve many lawful purposes, it also works to prevent law enforcement from using traditional IP identification techniques to investigate online crimes (such as the distribution of child pornography). (Doc. 29 at 2, n.2; Doc. 31 at 4, n.2).

---

<sup>2</sup> As the Government points out, “[t]here was no doubt what purpose Playpen served; from September 2014 until February 19, 2015, its login page contained two images depicting partially clothed prepubescent girls with their legs spread apart.” (Doc. 31 at 3).

<sup>3</sup> The federal investigation revealed that over 1,500 unique users visited the website daily and over 11,000 unique users visited the website per week. (Doc. 29, Ex. 3 at ¶ 19).

<sup>4</sup> Tor was originally developed by the United States Naval Research Laboratory for the primary purpose of protecting government communications. (Doc. 29, Ex. 3 at ¶ 7). However, Tor is now available to the public simply by downloading the software from the Tor website. (*Id.*)

In order to mask a user's IP address, Tor routes the user's communications through a network of relay computers located all over the world, rather than through a more direct connection. (*Id.*) Stated simply:

The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover [the user's] tracks so no observer at any single point can tell where the data came from or where it's going.

Why We Need Tor, Tor: Overview, <https://www.torproject.org/about/overview.html.en> (last visited on Nov. 20, 2016).<sup>5</sup>

Additionally, Tor allows users to utilize certain “hidden services,” which include hosting websites that are inaccessible to those not using Tor and, further, are hidden from those who do not know of the website's existence and precise Tor-based web address. (Doc. 31 at 4-5). Moreover, Tor masks the IP address of the server hosting these hidden websites and, accordingly, the location of the server cannot be determined. (*Id.*) Playpen was one such “hidden” website. (*Id.*)

However, in December 2014, a foreign law enforcement agency provided federal agents with an IP address suspected to belong to the server hosting Playpen. (Doc. 29, Ex. 3 at ¶ 28). Through further investigation, the Federal Bureau of Investigations (“FBI”) was able to verify the accuracy of the information and trace the IP address to a

---

<sup>5</sup> For example, when a user on the Tor network accesses a website, the IP address that appears in the website's IP log is that of a Tor “exit node” rather than the user's actual IP address. (Doc. 29, Ex. 3 at ¶ 8). An “exit node” is the last computer through which Tor routed the user's communication. (*Id.*) Thus, Tor's routing strategy obscures a user's true location, and there is no practical way to trace the user's actual IP back through the Tor exit node. (*Id.*)

server hosting company headquartered in North Carolina. (*Id.*) On February 20, 2015, federal agents seized the server from its location in North Carolina and took it to Virginia, where the FBI assumed administrative control over Playpen. (Doc. 29 at 2).

As part of a larger effort to identify registered users, the FBI allowed Playpen to continue in operation until March 4, 2015. (Doc. 31 at 5). To that end, federal prosecutors and agents in the Eastern District of Virginia (“EDVA”) proceeded to obtain two separate warrants. (*Id.*)

**First**, EDVA prosecutors obtained a Title III search warrant (the “Title III warrant”) from an EDVA district judge. (Doc. 29 at 3). The Title III warrant permitted investigators to intercept electronic communications exchanged between unknown “target subjects” or “unidentified administrators and users” on Playpen’s private chat and messaging services. (*Id.*) **Second**, EDVA agents obtained a search warrant from an EDVA magistrate judge, authorizing agents to use a Network Investigative Technique (“NIT”) to identify Playpen users (the “NIT warrant”). (*Id.* at 4).

Specifically, a NIT is an investigative method used to circumvent Tor’s anonymity features, thereby allowing law enforcement to identify the individuals who are visiting particular hidden websites. (Doc. 29, Ex. 3 at ¶¶ 31-35). In the affidavit in support of the NIT warrant application, the Affiant explained that:

In the normal course of operations, websites send content to visitors. A user’s computer downloads that content and uses it to display web pages on the user’s computer. Under the NIT ..., [Playpen], which will be located in Newington, Virginia [EDVA], would augment that content with additional computer instructions. When a user’s computer successfully downloads those instructions from [Playpen], in

the [EDVA], the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain [identifying] information to a computer controlled by or known to the government.

(*Id.* at ¶ 33). The identifying information to be transmitted included, *inter alia*, the computer's actual IP address, operating system and version, host name, active username, and unique media access control ("MAC") address. (*Id.* at ¶ 34). Further, the application in support of the NIT warrant specifically requested authorization to deploy the NIT in order to obtain the identifying information from "activating computers – wherever located...." (*Id.* at ¶ 46) (emphasis added).

EDVA agents obtained the NIT warrant and deployed the NIT on Playpen on February 20, 2015. (Doc. 29, Ex. 1 at ¶ 25). The NIT remained active, allowing EDVA agents to collect the identifying information of the registered users who logged into Playpen, until the website was taken offline on March 4, 2015.<sup>6</sup> (*Id.*)

As a result of the NIT, law enforcement obtained the identifying information of Playpen users, including one particular user who logged into Playpen on March 3, 2015

---

<sup>6</sup> As previously stated, Playpen was a hidden website on the Tor network, accessible only to registered Playpen users who were connected to the Tor network and who were privy to Playpen's precise Tor-based web address. Therefore, as an initial matter, it is highly unlikely that anyone would have accidentally stumbled unto Playpen. (*See* Doc. 29, Ex. 1 at ¶ 9). However, even assuming that some Tor users *had* accidentally come across Playpen, they still would not have been able to access Playpen's content unless and until they intentionally navigated past the prominently displayed child pornography on Playpen's homepage and deliberately registered as a Playpen user. (*Id.*; Doc. 31 at 3-4). In short, there is no doubt that the users identified by the NIT were knowingly and intentionally seeking out child pornography on Playpen.

under the name “torlayer.”<sup>7</sup> (Doc. 31 at 8). Law enforcement learned from the Internet Service Provider (Time Warner Cable) that the IP address used by “torlayer” to access Playpen was associated with Defendant Eric Schuster at 1500 Sherwood Drive, Apt. 4D, Fairfield, Ohio 45014 (the “Sherwood Drive residence”). (Doc. 29, Ex. 1 at ¶ 34). Agents verified that Defendant lived at the Sherwood Drive residence. (*Id.* at ¶ 35).

Based upon the foregoing information, on August 6, 2015, within the Southern District of Ohio (“OHSD”), a federal agent (the “OHSD affiant” or “OHSD agent”) obtained from a federal magistrate judge in this district (the “OHSD magistrate judge”), a warrant to search the Sherwood Drive residence (the “OHSD warrant”). (Doc. 29, Ex. 1). The OHSD warrant was executed on August 7, 2016. (Doc. 31 at 9). As a result of the search, a total of 18 items of evidence were seized including, *inter alia*, four internal hard drives, which contained thousands of images and videos of suspected child pornography and child erotica. (*Id.*)

## II. STANDARD OF REVIEW

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,” and, further, requires a showing of probable cause before a warrant may issue. U.S. Const. amend. IV. “The exclusionary rule prohibits the admission of evidence seized in searches and seizures that are deemed unreasonable under the Fourth Amendment, as well as derivative evidence acquired as a result of an unlawful search.” *United States v.*

---

<sup>7</sup> Federal agents were able to determine the IP address used by “torlayer” to access Playpen, the unique MAC address of the network adapter used by “torlayer,” and that the computer used by “torlayer” had the host name “Eric-PC” and the log-on name “Eric.” (Doc. 29, Ex. 1 at ¶ 28).

*Kennedy*, 61 F.3d 494, 497 (6th Cir. 1995) (citing *Wong Sun v. United States*, 371 U.S. 471, 484-85 (1963)). The purpose of the exclusionary rule is to deter law enforcement from obtaining evidence through unconstitutional means. *Nix v. Williams*, 467 U.S. 431, 442-43 (1984).

A defendant may seek the suppression of evidence by filing a pretrial motion with the court. Fed. R. Crim. P. 12(b)(3)(C) and 41(h). “It is well settled that in seeking suppression of evidence the burden of proof is upon the defendant to display a violation of some constitutional or statutory right justifying suppression.” *United States v. Patel*, 579 F.App’x 449, 453 (6th Cir. 2014) (quoting *United States v. Rodriguez–Suazo*, 346 F.3d 637, 643 (6th Cir.2003)).

### III. ANALYSIS

Defendant moves to suppress “the evidence obtained as a result of the issuance of the NIT Warrant, arguing that the NIT Warrant is void for want of jurisdiction under the Federal Magistrates Act, 28 U.S.C. § 636(a), and additionally that it violated Federal Rule of Criminal Procedure 41(b).” (Doc. 29 at 1). Defendant further argues that the good-faith exception under *United States v. Leon*, 468 U.S. 897 (1984), does not apply. (*Id.* at 13-19).

Conversely, the Government argues that Defendant’s motion should be denied because Defendant did not have a reasonable expectation of privacy in his IP address and therefore no search occurred. (Doc. 31 at 10-13). Further, the Government argues that, even assuming that a search did occur, the magistrate judge had authority under Fed. R. Crim. P. 41(b) to issue the warrant. (*Id.* at 13-15). Alternatively, the Government asserts

that, should the Court find issuance of the NIT warrant violated Rule 41, suppression is not the appropriate remedy. (*Id.* at 15-17). Finally, the Government argues that, regardless of the circumstances, suppression is not warranted because the *Leon* good-faith exception applies. (*Id.* at 20).

Before deciding whether a Fourth Amendment violation occurred, the Court may choose to determine first whether the exclusionary rule applies. “[C]ourts could reject suppression motions posing no important Fourth Amendment questions by turning immediately to a consideration of the officers’ good faith.” *Leon*, 468 U.S. at 925. Whether it is necessary to address the Fourth Amendment question posed in a particular case is within the “informed discretion” of the Court. *Id.*

Here, the Court finds that there is no basis to resolve the Fourth Amendment issues before turning to the good-faith analysis.<sup>8</sup> Specifically, while Defendant’s motion to suppress poses a complex and multi-faceted series of technical questions, the resolution of which has perplexed district courts across the country, the underlying issue has since been entirely resolved by amendment of the Federal Rules of Criminal Procedure. See Fed. R. Crim. P. 41(b) (2016), *amended by* Fed. R. Crim. P. 41(b)(6)

---

<sup>8</sup> To be clear, the Court’s finding does not imply that violation of an individual’s Fourth Amendment rights ever lacks importance. Rather, the focus of importance, as referenced in *Leon*, is on the area of Fourth Amendment jurisprudence, such as where “resolution of a particular Fourth Amendment question is necessary to guide future action by law enforcement officers and magistrates.” *Leon*, 468 U.S. at 925.



(Dec. 1, 2016).<sup>9</sup> Therefore, the Court finds that resolution of the Fourth Amendment issues serves no value to Fourth Amendment jurisprudence, as the potential risk of harm is no longer capable of repetition.

Accordingly, the Court declines to begin its analysis by addressing the specific Fourth Amendment issues raised in Defendant’s motion. Instead, the Court turns to the question—whether the agents acted in good-faith in obtaining and executing the warrants at issue. As fully stated below, the Court finds that the agents **did** act in good-faith and that the exclusionary rule **does not** apply.

“The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies.”

*Herring v. United States*, 555 U.S. 135, 140 (2009). Indeed, “[t]he Fourth Amendment contains no provision expressly precluding the use of evidence obtained in violation of its commands ....” *Leon*, 468 U.S. at 906. And the Supreme Court has “repeatedly rejected

---

<sup>9</sup> The amendment to Rule 41(b), effective December 1, 2016, added subsection (6), and states as follows:

(b) Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:

...

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

the argument that exclusion is a necessary consequence of a Fourth Amendment violation.” *Herring*, 555 U.S. at 141 (noting that “**exclusion ‘has always been our last resort, not our first impulse’**” (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006) (emphasis added))).

In that regard, “[t]he purpose of the exclusionary rule is not to redress the injury to the privacy of the search victim: ‘[T]he ruptured privacy of the victims’ homes and effects cannot be restored. Reparation comes too late.’” *United States v. Calandra*, 414 U.S. 338, 347 (1974) (quoting *Linkletter v. Walker*, 381 U.S. 618, 637 (1965)). Instead, “the [exclusionary] rule is a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved.” *Id.* at 348. In other words, “[t]he rule is calculated to prevent, not to repair. Its purpose is to deter—to compel respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard it.” *Elkins v. United States*, 364 U.S. 206, 217 (1960).

“As with any remedial device, the [exclusionary] rule’s application has been restricted to those instances where its remedial objectives are thought most efficaciously served.” *Arizona v. Evans*, 514 U.S. 1, 11 (1995). Courts must therefore make a case-by-case determination and grant suppression “only in those unusual cases in which exclusion will further the purposes of the exclusionary rule.” *Leon*, 468 U.S. at 918 (emphasis added).

In particular, the “‘prime purpose’ of the exclusionary rule ‘is to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment

against unreasonable searches and seizures.’” *Illinois v. Krull*, 480 U.S. 340, 347 (1987) (quoting *Calandra*, 414 U.S. at 347). More specifically, “the exclusionary rule serves to deter **deliberate, reckless, or grossly negligent conduct**, or in some circumstances recurring or systemic negligence.” *Herring*, 555 U.S. at 144 (emphasis added). Indeed, even “when police mistakes are the result of negligence ... rather than systemic error or reckless disregard of constitutional requirements, any marginal deterrence does not ‘pay its way’ ... [and therefore], the criminal should not ‘go free because the constable has blundered.’” *Id.* at 147-48 (quoting *People v. Defore*, 150 N.E. 585, 587 (N.Y. 1926)). In short, “[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” *Herring*, 555 U.S. at 144.

“‘[A] warrant issued by a magistrate normally suffices to establish’ that a law enforcement officer has ‘acted in good faith in conducting the search.’” *Leon*, 468 U.S. at 922 (quoting *United States v. Ross*, 456 U.S. 798, 823, n. 32 (1982)). Thus, “[c]ourts should not ... suppress ‘evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant.’” *United States v. Carpenter*, 360 F.3d 591, 595 (6th Cir. 2004) (quoting *Leon*, 468 U.S. at 922). Significantly, “the exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates.” *Leon*, 468 U.S. at 916 (emphasis added).

Of course, an “officer’s reliance on the magistrate’s probable-cause determination and on the technical sufficiency of the warrant [that the magistrate judge] issue[d] must be objectively reasonable ....” *Id.* at 922. Indeed, the exclusionary rule will “not apply

in cases where the issuing magistrate wholly abandoned his judicial role ... [if under] such circumstances, no reasonably well trained officer should rely on the warrant.” *Id.* at 923.

However, “[i]n the ordinary case, an officer cannot be expected to question the magistrate’s probable-cause determination or his judgment that the form of the warrant is technically sufficient ... [and] [p]enalizing the officer for the magistrate’s error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations.” *Id.* at 922. Accordingly, “evidence should be suppressed ‘only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment.’” *Krull*, 480 U.S. at 348-49 (quoting *United States v. Peltier*, 422 U.S. 531, 542 (1975)).

#### **A. The OHSD Warrant**

As an initial matter, the question presently before the Court is whether the evidence against Defendant in the instant case should be suppressed pursuant to the exclusionary rule. It therefore bears noting that the evidence at issue in the instant case was seized from Defendant’s home during the execution of the OHSD warrant. Thus, the Court finds the parties’ emphasis on the validity of the EDVA NIT warrant (as opposed to the OHSD warrant) is misplaced.

In resolving whether to exclude evidence obtained during the execution of the OHSD warrant, the Court finds that the proper focus is on the propriety of the OHSD warrant. Unquestionably, the NIT warrant will factor into the Court’s analysis of the OHSD warrant (*i.e.*, as the source of the probable cause upon which the OHSD warrant

was issued). And the Court further acknowledges that it “must consider the actions of all the police officers involved.” *Herring*, 555 U.S. 140 (citing *Leon*, 468 U.S. at 923, n. 24 (“It is necessary to consider the objective reasonableness, not only of the officers who eventually executed a warrant, but also of the officers who originally obtained it or who provided information material to the probable-cause determination”))). Regardless, the question before the Court remains whether any deficiency exists as to the OHSD warrant, which would require exclusion of the evidence obtained during its execution. In that regard, this Court can simply assume, without deciding, that the EDVA magistrate judge lacked authority to issue the NIT warrant.

Focusing on the OHSD warrant, and assuming the NIT warrant is void because the EDVA magistrate judge lacked authority for its issuance, the Court must look to “whether there was good faith on the part of the agents.” (Doc. 33 at 5:17-6:7). Defendant argued during oral arguments that the OHSD affiant is “an experienced FBI agent who is familiar with what happened in [EDVA], is familiar with Rule 41,” and regardless of jurisdiction “should have known ... that the [NIT] warrant was invalid.” (*Id.* at 6:10-16). More specifically, Defendant argued that, because Defendant is not the first to challenge the NIT warrant in the context of the Playpen investigation, the OHSD agent should have known the NIT warrant was invalid. (*Id.* at 7:1-25). Additionally, Defendant asserts that the agents should have been aware that the NIT warrant was not authorized under Rule 41(b), as written at the time, because “[a] memorandum addressed to the Committee on Rule of Practice and Procedure dated May 5, 2014, introduce[d] [the] proposed amendment to Rule 41(b) that would authorize the use of the NIT

Warrant.” (Doc. 29 at 18). Defendant alleges that holding the agent to such high standards of legal knowledge is in line with *Leon* and accomplishes the purpose of the exclusionary rule—that “the lesson is to be sent to the [agents] ....” (Doc. 33 at 6:19-25). The Court rejects Defendant’s position.

First, the EDVA agents obtained the NIT warrant on February 20, 2015, and the NIT remained active on the Playpen server until March 4, 2015. (Doc. 29, Ex. 1 at ¶ 25). Just five months later, on August 6, 2015, the OHSD agent obtained the OHSD warrant. (*Id.* at Ex. 1). And while Defendant argues that the OHSD agent should have known that the NIT warrant was invalid because of the ongoing challenges by other defendants, this Court is unable to find any case arising from the Playpen investigation where a motion challenging the NIT warrant predates the August 6, 2015 OHSD warrant.<sup>10</sup>

Second, the Court rejects Defendant’s argument that the agents were on notice that the NIT warrant may be invalid, based on the existence of a memorandum, to the Judicial Conference Committee on Rule of Practice and Procedure, proposing the amendment to Rule 41(b), just a few months before the NIT warrant was obtained.<sup>11</sup> The Court finds it entirely unreasonable to hold agents to such a standard of knowledge.

---

<sup>10</sup> The earliest challenge to the NIT warrant that this Court was able to find came out of a case from the Western District of Washington. *United States v. Michaud*, No. 3:15-cr-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). In *Michaud*, the defendant’s motion to suppress was filed in October 2015, and was decided in January 2016. (*Id.*) However, even if an earlier case exists, it is unreasonable to expect federal agents to find such a case when even this Court is unable to do so.

<sup>11</sup> While Defendant cites to the memorandum as being dated May 5, 2014, it appears that the memorandum was revised in July 2014, and was only distributed in preliminary form on August 15, 2014. See Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure, <http://www.fpd-ohn.org/node/778>.

Indeed, if *anyone* should have been charged with such specific legal knowledge, it would have been the magistrate judges, not the agents.

Beyond the argument that the agents essentially ‘should have known better,’ there is no evidence that any agent acted unreasonably, let alone deliberately or recklessly.

Indeed, the sheer number of agents who have relied upon the NIT warrant, and obtained subsequent warrants from magistrate judges in their own jurisdictions, as well as the inconsistent rulings by district courts across the country, shows that no aspect of the NIT warrant’s validity constitutes a simple question nor a close call.<sup>12</sup> Accordingly, it is unreasonable to expect either the EDVA agent or the OHSD agent to have concluded,

---

<sup>12</sup> Some courts have found that the EDVA magistrate judge lacked authority to issue the NIT warrant and, further, found suppression to be the appropriate remedy. *E.g.*, *United States v. Workman*, 205 F. Supp. 3d 1256 (D. Colo. Sept. 6, 2016). Other courts have determined that the EDVA magistrate judge lacked authority, but have declined to suppress the evidence based on the good-faith exception. *E.g.*, *United States v. Ammons*, No. 3:16-CR-00011-TBR-DW, 2016 WL 4926438, at \*9 (W.D. Ky. Sept. 14, 2016). Still other courts have found that the EDVA magistrate judge had authority to issue the NIT warrant pursuant to Rule 41(b)(4)’s tracking device provision. *E.g.*, *United States v. Matish*, 193 F. Supp. 3d 585, 612-13 (E.D. Va. May 5, 2016). Moreover, among the courts that found the issuance of the NIT warrant to have violated Rule 41(b), there is further disagreement as to whether the violation was constitutional or technical in nature, and still whether suppression is appropriate in either circumstance. *Compare United States v. Henderson*, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at \*4 (N.D. Cal. Sept. 1, 2016) (holding “suppression is not appropriate because the violation was technical, not constitutional...”), with *United States v. Croghan*, No. 1:15-CR-48, 2016 WL 4992105, at \*7 (S.D. Iowa Sept. 19, 2016) (“Assuming that the Rule 41(b) violation was merely technical, the Court would still find suppression appropriate ...”), *United States v. Werdene*, 188 F. Supp. 3d 431, 447–48 (E.D. Pa. May 18, 2016) (“Even if ... the Rule 41(b) violation [were] constitutional in nature—suppression is not the appropriate remedy”), and *United States v. Levin*, 186 F. Supp. 3d 26, 42 (D. Mass. 2016) (“[because] the conduct at issue here can be described as ‘systemic error or reckless disregard of constitutional requirements,’ ... suppression is appropriate”). Further still, there is even disagreement among the district courts as to whether the NIT constituted a ‘search’ at all. *Compare United States v. Acevedo-Lemus*, No. SACR 15-00137-CJC, 2016 WL 4208436, at \*4 (C.D. Cal. Aug. 8, 2016) (holding the NIT’s acquisition of Defendant’s IP address was not a search because “Defendant could not have had a subjective expectation of privacy in his IP address” and “[s]ociety [d]oes [n]ot [r]ecognize Defendant’s [e]xpectation as [r]easonable”), with *United States v. Darby*, 190 F. Supp. 3d 520, 530 (E.D. Va. June 3, 2016) (“The government’s deployment of the NIT was a Fourth Amendment search”).

contrary to the findings of the magistrate judges, that the NIT warrant was invalid. *See Leon*, 468 U.S. at 922 (“In the ordinary case, an officer cannot be expected to question the magistrate’s probable-cause determination or his judgment that the form of the warrant is technically sufficient”); *Massachusetts v. Sheppard*, 468 U.S. 981, 989–90 (1984) (“we refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested”).

Thus, the Court finds the exclusionary rule inapplicable here, as there is no basis upon which to conclude that any agent involved in the Playpen investigation, or any derivative investigation, knew or should have known that the validity of the NIT warrant, or any subsequently obtained warrant, was unconstitutional or procedurally improper. *See Krull*, 480 U.S. at 348-49 (“evidence should be suppressed ‘only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment’”) (quoting *Peltier*, 422 U.S. at 542). Moreover, there is no evidence that any agent engaged in “**deliberate, reckless, or grossly negligent conduct** ....” *See Herring*, 555 U.S. at 144 (emphasis added). Indeed, the simple fact alone, that district courts are unable to reach a firm consensus as to the validity of the NIT warrant, undermines any argument that the OHSD agent’s (or any agent’s) reliance on the NIT warrant was deliberate, reckless, or part of a “recurring or systemic negligence.” *Id.*; *see also Ammons*, 2016 WL 4926438, at \*9 (“The FBI agents can hardly be faulted for failing ‘to understand the intricacies of the



jurisdiction of federal magistrates’ ... After all, there is disagreement among reasonable jurists on that very question”) (quoting *Darby*, 190 F. Supp. 3d at 538).

In short, this Court finds it unreasonable to expect any agent to have made a definitive finding of law as to the NIT warrant, when magistrate judges and district judges across the nation have been and are unable to do so. Accordingly, the Court finds that the OHSD affiant acted in good-faith in relying upon the results of the NIT warrant as the basis for probable cause, as well as relying upon the findings of the OHSD magistrate judge as to the validity of the NIT and the OHSD warrants. Therefore, the exclusionary rule does not apply and suppression is not warranted.

## **B. NIT Warrant**

Despite the Court’s focus on the OHSD warrant, the Court feels compelled to also separately address the NIT warrant, in light of Defendant’s argument that the good-faith exception should not apply. Specifically, Defendant argues that, because the EDVA magistrate judge lacked authority to issue the NIT warrant, it is void *ab initio*. (Doc. 29 at 13-19). Accordingly, Defendant suggests that the Court should treat the NIT as a warrantless search and, citing to the Sixth Circuit’s decision in *United States v. Scott*, 260 F.3d 512 (6th Cir. 2001), argues that the good-faith exception does not apply.<sup>13</sup>

The Court finds Defendant’s reliance on *Scott*, for the proposition that the good-faith exception does not apply, wholly unpersuasive in light of the fact that the Sixth Circuit subsequently acknowledged in *United States v. Master* that “the Supreme Court’s

---

<sup>13</sup> Defendant further cites to numerous out-of-circuit cases, as well as state court opinions, which are neither binding on this Court nor persuasive in this context. (See Doc. 29 at 14 n.7).

evolving suppression rulings in Fourth Amendment cases require clarification or modification of our precedent in *Scott*.” 614 F.3d 236, 243 (6th Cir. 2010). The Sixth Circuit recognized, in light of the Supreme Court’s more recent decisions in *Herring*, 555 U.S. 135 and *Hudson* 547 U.S. 586, that in cases where a warrant is issued by a judge lacking legal authority, *Scott*’s categorical foreclosure of the good-faith exception is no longer viable. *Master*, 614 F.3d at 241-42. Rather, the Sixth Circuit explained that, “[t]he Supreme Court has effectively created a balancing test by requiring that in order for a court to suppress evidence following the finding of a Fourth Amendment violation, ‘the benefits of deterrence must outweigh the costs.’” *Id.* at 243 (quoting *Herring*, 555 U.S. at 141).

Accordingly, this Court finds that the good-faith exception is not rendered automatically inapplicable simply because law enforcement officers relied upon a warrant that is subsequently found to be void *ab initio*.<sup>14</sup> Therefore, even if this Court were to find that the EDVA magistrate judge lacked authority to issue the NIT warrant in the first instance, the Court could still turn to the “balancing test” to determine whether application of the exclusionary rule is warranted.

---

<sup>14</sup> Notably, in *Herring*, law enforcement seized evidence from the defendant’s person, incident to arrest, which arrest was conducted based upon the officers’ belief that the defendant had an outstanding warrant. 555 U.S. at 137. However, subsequent to the search, and after finding contraband and a weapon in the defendant’s pocket and in his vehicle, the officers learned that the warrant they believed to be outstanding had been recalled five months prior. *Id.* at 137-38. The Supreme Court found that “the conduct at issue was not so objectively culpable as to require exclusion ... when [the] evidence [was] obtained in objectively reasonable reliance on a subsequently recalled warrant.” *Id.* at 146. This Court finds the circumstances in *Herring* to be substantively akin to those in the instant case, as it can be argued that, in both instances, there was no warrant in place to justify law enforcement conduct.

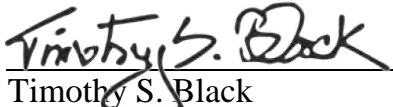
Accordingly, here, the Court follows the Supreme Court's clear instruction that the exclusionary rule is only applicable, **as a last resort**, to deter police misconduct. In doing so, and as previously stated, the Court finds no basis to conclude that the EDVA agents acted deliberately or recklessly in either obtaining or relying upon the NIT warrant. Rather, any deficiency in the NIT warrant was the result of judicial error, not law enforcement misconduct. Accordingly, the exclusionary rule serves no purpose and its application is therefore unwarranted.

## V. CONCLUSION

Based upon the foregoing, Defendant's motion to suppress (Doc. 29) is **DENIED**.

**IT IS SO ORDERED.**

Date: March 28, 2017

  
Timothy S. Black  
United States District Judge